Defensive Information Warfare Branch Presentation

C. Maciag
Air Force Research Laboratory
AFRL/IFGB
525 Brooks Rd.
Rome, NY 13441-4505
United States

In the interests of readability and understandability, it is RTO policy to publish PowerPoint presentations only when accompanied by supporting text. There are instances however, when the provision of such supporting text is not possible hence at the time of publishing, no accompanying text was available for the following PowerPoint presentation.

Click here to view PowerPoint presentation; Press Esc to exit

Discussion – Paper 21

DISCUSSION AM 8 JUN 2000

The subjects were raised as a result of the presentations made by Chet Macaig about Information Operations. Answers by Chet unless otherwise annotated.

Q 1

The problem of detecting attacks of information systems is complicated by the number of false positives which have to be filtered by humans.

A

Sensors do not have a refined enough view to directly detect an attack. However, attacks have a purpose and therefore a sequence of events. It is this sequence that needs to be identified. MIT have developed Bottle neck verification techniques to do this, it looks at business flows and identifies anomalies within. An example of the ways in which in UNIX there are 2/3 authorised ways to go from normal to super user, any other method would be an anomaly. Key to identifying these may be the use of neural networks to ascribe a probability of the behaviour being divergent.

Q2 What sort of information was being shared.

A

Overall goal was to have a common visualisation by all 4 countries involved in the collaboration. Sharing was complex because o the lack of interoperability of visualisation tools. Auto correlation techniques used for RADAR target extraction has interesting possibilities in this new domain.

Paper presented at the RTO IST Workshop on "Multimedia Visualization of Massive Military Datasets", held in Quebec, Canada, 6-9 June 2000, and published in RTO-MP-050.

Milan Kuchta added: Ontologies and data sharing within an international sphere has always been a politically difficult. The technology is not the whole problem. As we enter this new space we need to take with us the survival skills that have evolved and kept us safe in our normal environment. How we take these tools into the new space is the key question. Underlying approach analogous to biological evolution, we need to take our best weapons and then learn how to make them better, and fast! Forensics give another good example to learn from, they do not need to know everything about the criminal you only need a finger print.

Statement from Bill Wright: in investigating cellular telephone fraud visualisation techniques have been developed to identify deviant behaviour.

Q From the Chair: Have architectural Portals been investigated

A No

Then clarification on the definition of Portal as a single specific view.

A

Not customized visualisation but customisable visualisation is required. Similar to some of the internet tools e.g. YAHOO.

Lengthy discussion about Portals, semantics and transformations. Interaction through Portals must preserve the integrity of the information, not the data.